BAB IV

PENUTUP

4.1. Kesimpulan

Penelitian ini membuktikan bahwa meningkatnya kejahatan *phishing* di Singapura tidak dapat disebabkan semata-mata sebagai akibat dari kecanggihan teknologi pelaku atau kelemahan sistem dalam keamanan perbankan. Sebaliknya, penelitian ini menunjukkan bahwa serangan *phishing* berhasil karena adanya faktor non-teknis khususnya praktik *social engineering* yang mengeksploitasi aspek psikologis dan perilaku pengguna layanan perbankan digital. Melalui manipulasi kepercayaan, penciptaan rasa urgensi, serta penyamaran identitas yang menyerupai institusi resmi, pelaku *phishing* mampu memengaruhi respons pengguna sehingga perlindungan teknis yang ada tidak selalu efektif dalam mencegah terjadinya penipuan. Hal ini menunjukkan bahwa ancaman *phishing* perlu dipahami sebagai persoalan keamanan siber yang tidak hanya bersifat teknologis, tetapi juga berkaitan erat dengan dimensi sosial dan perilaku pengguna.

Sejalan dengan temuan tersebut, penelitian ini menunjukkan bahwa peran *Cyber Security Agency of Singapore* (CSA) dalam upaya pencegahan ancaman *phishing* di Singapura telah dilakukan melalui pendekatan yang relatif komprehensif, baik melalui penguatan kebijakan teknis maupun melalui strategi non-teknis berupa *Cybersecurity Awareness Campaign* dalam program kampanye "*Better Cyber Safe than Sorry*". Kampanye CSA ini menempatkan edukasi dan peningkatan kesadaran publik sebagai bagian penting dari strategi keamanan siber nasional Singapura, dengan tujuan membentuk perilaku digital yang lebih aman di kalangan pengguna layanan perbankan. Pendekatan ini mencerminkan penerapan konsep *cyber resilience*, di mana keamanan siber tidak hanya dipahami sebagai upaya pencegahan serangan, tetapi juga sebagai kemampuan untuk menghadapi, beradaptasi, dan memulihkan fungsi sistem serta kepercayaan publik ketika serangan *phishing* terjadi. Namun demikian, hasil penelitian menunjukkan bahwa efektivitas kampanye tersebut masih menghadapi tantangan, khususnya dalam memastikan bahwa peningkatan pengetahuan pengguna benar-benar terinternalisasi dalam praktik penggunaan layanan perbankan digital sehari-hari.

Dengan demikian, penelitian ini berangkat dari pertanyaan utama mengenai bagaimana *Cybersecurity Awarness Campaign "Better Cyber Safe than Sorry"* oleh CSA di Singapura di tinjau dari konsep *Cyber Resilience* dan *Social engineering*. Pertanyaan tersebut dijawab dengan temuan bahwa CSA menangani *phishing* melalui penguatan kebijakan keamanan siber, peningkatan literasi digital masyarakat melalui kampanye *"Better Cyber Safe than Sorry"*. Namun, penelitian ini menunjukkan bahwa pendekatan tersebut masih menghadapi tantangan karena peningkatan literasi digital belum sepenuhnya diikuti oleh perubahan perilaku pengguna secara konsisten, sementara karakter serangan *phishing* yang adaptif dan berbasis manipulasi perilaku terus berkembang. Kondisi ini menuntut penguatan integrasi antara kebijakan teknis dan strategi literasi digital agar penanganan *phishing* dapat berjalan lebih efektif dan berkelanjutan.

4.2. Saran

Berdasarkan temuan dan analisis yang telah dipaparkan dalam penelitian ini, terdapat beberapa saran yang dapat diajukan dalam ranah kebijakan, institusional, masyarakat, regional, serta penelitian selanjutnya. Saran-saran ini bertujuan untuk memperkuat upaya penanganan kejahatan *phishing* di Singapura agar tidak hanya berfokus pada respons teknis, tetapi juga mampu membangun ketahanan digital yang lebih menyeluruh dan berkelanjutan.

Pertama, *Cyber Security Agency of Singapore* (CSA) perlu untuk memperkuat koordinasi kebijakan dalam penanganan *phishing* di Singapura. Hasil penelitian menunjukkan bahwa upaya penanganan *phishing* selama ini masih lebih menekankan aspek teknis dan edukasi secara terpisah, sehingga dampaknya sangat bergantung pada kesiapan masing-masing pihak. Kondisi ini membuat respons terhadap *phishing* belum selalu berjalan selaras antara kebijakan, praktik perbankan, dan perlindungan pengguna. Oleh karena itu, CSA perlu mendorong koordinasi yang lebih jelas dan konsisten agar pembelajaran dari kasus *phishing* dapat langsung diterapkan dalam prosedur operasional perbankan.

Kedua, kampanye *"Better Cyber Safe than Sorry"* perlu terus dikembangkan agar tidak hanya meningkatkan pengetahuan, tetapi juga mendorong perubahan perilaku pengguna. Hasil penelitian menunjukkan bahwa meskipun masyarakat sudah semakin mengetahui risiko *phishing*, hal tersebut belum selalu diikuti dengan sikap yang lebih waspada saat menggunakan layanan perbankan digital. Oleh karena itu, CSA perlu menyampaikan pesan kampanye dengan cara yang lebih praktis dan dekat dengan pengalaman sehari-hari pengguna, misalnya melalui contoh kasus penipuan yang sering terjadi atau simulasi sederhana, agar pesan keamanan siber lebih mudah dipahami dan diterapkan.

Ketiga, industri keuangan di Singapura perlu berperan lebih aktif dalam upaya pencegahan dan penanganan *phishing*. Industri keuangan tidak hanya berfungsi sebagai penyedia layanan keuangan, tetapi juga memiliki peran penting dalam membentuk kebiasaan digital nasabah. Oleh karena itu, perlunya memperkuat edukasi kepada nasabah, menyampaikan informasi secara terbuka ketika terjadi insiden, serta menyediakan saluran pelaporan yang mudah dan cepat. Langkah-langkah ini penting untuk mengurangi dampak *phishing* dan menjaga kepercayaan masyarakat terhadap layanan digital.

Keempat, bagi peneliti selanjutnya, disarankan untuk melakukan kajian lapangan melalui wawancara langsung dengan *Cyber Security Agency of Singapore* (CSA) sebagai institusi utama dalam penanganan keamanan siber. Meskipun dalam praktiknya akses informasi sering dilakukan melalui pihak perantara, penelitian lanjutan diharapkan dapat menggali perspektif CSA secara langsung agar pemahaman mengenai perumusan kebijakan, strategi literasi digital, serta tantangan penanganan *phishing* dapat diperoleh secara lebih optimal. Selain itu, wawancara dengan organisasi masyarakat sipil atau NGO di Singapura juga penting untuk melihat bagaimana program keamanan siber, termasuk kampanye *"Better Cyber Safe than Sorry"*, diimplementasikan di lapangan dan dirasakan dampaknya oleh masyarakat pengguna layanan digital.